Course Mechanics

- 30% HW (every 2 weeks?)
- 30% midterm (tentatively November 17)
- 30% final project
- 10% intangibles

No TA - you will (communally) grade a HW.

Cryptography:

- Part of (but not all) of security
- A fun application: math
- A fun sub-area of theoretical CS

Topics

- History (today)
- Proper definitions, security reductions
- Symmetric key crypt: stream cipher, block cipher
- Integrity: MACs, hash functions
- Public-key crypto: encryption, signatures
- Fun topics: secret sharing, commitments, zero-knowledge proofs

Background:

re: crypto/math: basic probability, little amount algebra/number theory, reductions + proofs

coding: there will be coding
Historical Ciphers

Caesar Cipher 100 - 44 BC

plaintext A B C D . . . . . U X Y Z
shift 3 3 3 3

Ciphertext D E F G . . . . . Z A B C

Auguste Caesar changed key from D to L
Generalization: shift cipher
Crypthonysis:
1. Brute force: only 26 possible keys
2. Frequency analysis: recognize letter distribution of English

Still use!

2006: Mafia boss Bernardo Provenzano uses Caesar cipher
(enforced w/ numbers)

2011: Rajib Karim plotted to blow up BA planes w/ Bangladeshi actwists
Excel Caesar cipher (rejected more modern cryps being "not behin
known today as most secure")

Encryption Syntax:

\[
\begin{align*}
\text{Alice} & \rightarrow \text{Bob} \\
\text{m} & \rightarrow \text{Enc}_k(m) \\
\text{Enc}_k(m) & \rightarrow \text{c} \\
\text{c} & = \text{Enc}_k(m) \\
\text{Dec}_k & \rightarrow \text{m} \\
\text{Dec}_k(\text{c}) & = \text{m} \\
\text{satisfying Dec}_k(\text{Enc}_k(m)) & = m
\end{align*}
\]

Exercise: Formulate Caesar cipher.

Kerckhoffs' Principle (Auguste Kerckhoffs 1883)
"The cipher must not be required to be secret, and it must be safe to fall into the hands of the enemy without inconvenience."
- Encryption scheme should not be secret
- only key needs to be kept secret

Modern interpretation:
- Algorithm should be public, standardized, and scrutinized publicly.
“Sufficient key space principle”
Any secure encryption scheme must have a key space that is not reducible to an exhaustive search.
- Necessary but not sufficient

Mono-alphabetic substitution
plain: abc d
cipher: E UA A

What's its keys? \(26! \approx 2^{88.6}\)
How to break?
- Frequency analysis

Vigenère Cipher  "poly-alphabetic shift"
Giovanni Battista Bellaso in 1553
ascribed to Blaise de Vigenère - French Diplomat

plaintext: TO BE OR NOT TO BE
key: run run run run run
cipher: KLOVIEEGCIOV

Cryptanalysis:
If know key length \(n\):
1. Break cipher text into \(n\)
2. Solve each slice as Caesar cipher

How to find \(n\)?
Kasiski method  (Friedrich Kasiski 1863)
Repeating strings essentially encrypted same key letters
\(\text{dist gcd repeated cipher text strings} \approx \text{mult of key length} \) \(2009: \text{Jacob Appelbaum finds circuviation tool Psiphon using a Vigenère cipher}
\text{Psiphon.ca/node/125 "XOR cipher" (fix still broken)}
What is a strong pseudorandom function? (And perfectly random)

One-Time Pad
Gen: \( k \in \{0,1\}^n \) uniform
Enc: \( k \in \{0,1\}^n, m \in \{0,1\}^n \rightarrow c = k \oplus m \)
Dec: \( m = c \oplus k \)

What does “secure” mean?

1. No adversary can compute secret key from ciphertext.
2. No adversary can compute plaintext from ciphertext.
3. No adversary can determine a character of plaintext.
4. Meaningful information?
5. Can’t compute any function of plaintext from ciphertext.

Def. “perfect secrecy”
for every probability distribution over \( \{ m \} \)
\( \forall m \in \{ m \} \), \( \forall c \in \{ c \} \)
\( \Pr[M = m | C = c] = \Pr[M = m] \) \( \iff \Pr[C = c | M = m] = \Pr[C = c] \)

Lem. “perfect indistinguishability”
ciphertext scenario perfectly secret \( \iff \) ciphertext-only attack
for every probability distribution over \( \{ m \} \)
\( \forall m_0, m \in \{ m \} \), \( \forall c \in \{ c \} \)
\( \Pr[C = c | M = m_0] = \Pr[C = c | M = m] \)

Proof \( \Rightarrow \)
\(| \Pr[C = c | M = m_0] = \Pr[C = c | M = m] \)
\( \iff \Pr[C = c] = \sum_{m_0} \Pr[C = c | M = m_0] \cdot \Pr[M = m_0] \)
\( = \sum_{m} \Pr[C = c | M = m] \cdot \Pr[M = m] \)
\( = \Pr[C = c | M = m] \) \( \iff \) true for any \( m_0 \)

Thus OTP is perfectly secret
\( \Pr[C = c | M = m] = \frac{1}{2} \Pr[M = m] = \frac{1}{2} \Pr[k = m \oplus c] = \frac{1}{2} \)
\( \iff \) for any \( m_0, m \), \( \Pr[C = c | M = m_0] = \frac{1}{2} = \Pr[C = c | M = m] \)
Let $(Gen, Enc, Dec)$ be a perfectly secret encryption scheme

$$\Rightarrow |k| \leq |M| \quad k \in \mathcal{K} \quad M \in \mathcal{M}$$

**Pf**

Show if $|k| < |M| \Rightarrow m$ is perfectly secret.

Fix uniform distribution $M$.

Let $M(c) = \{m \mid m = Dec_k(c) \text{ for some } k \in \mathcal{K}\}$

$|M(c)| \leq |k| \Rightarrow \exists m' \in M \text{ s.t. } m' \in M(c)$

$$Pr[M = m' \mid C = c] = 0 \neq Pr[M = m']$$